UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/814,680	03/19/2001	Marius Constantin Ionescu		6558

7590 08/02/2004

Paul D. Gornall
Barrister & Solicitor
Reg'd Patent & TM Agent
1820 - 355 Burrard St.
Vancouver, V6C 2G8
CANADA

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/814,680	IONESCU, MARIUS CONSTANTIN	
	Examiner	Art Unit	
	Beemnet W Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 have been examined.

Claim Objections

2. Claims 1, 3, 19 and 20 are objected to because of the following informalities: a period is missing at the end of each claim. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,9,10,17, and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by De Jong et al. (hereinafter refereed to as De Jong) (US Patent No. 6,553,351 B1).

5. As per claim 1, De Jong teaches an authentication and data security system for communications in which

a communication key is derived by a first party subsystem using an encryption algorithm from key data previously provided by a second party subsystem to the first party subsystem [column 3, lines 30-47 and column 4, lines 9-24];

the communication key is transmitted to the second party subsystem, which uses a decryption algorithm to check whether the communication key was derived from any of various key data from a previously provided data pool related to the first party subsystem [column 3, lines 30-47, column 4, lines 9-24, lines 35-47].

6. As per claim 9, De Jong teaches the system as applied to claim 1 above. Furthermore, De Jong teaches the system in which the encryption algorithm is dynamic [column 4, lines 60-67 and column 5, lines 1-16].

7. As per claim 10, De Jong teaches the system as applied above. Furthermore, De Jong teaches the system in which the encryption algorithm is a context dependent dynamic cryptosystem [column 4, lines 60-67 and column 5, lines 1-16].

8. As per claim 17, De Jong teaches the system as applied above. Furthermore, De Jong teaches the system in which the communication key for a specific communication session is derived from the key data in combination with a parameter based on an incremented number related to the current communication session in a series of communications between the first and second parties [column 9, lines 1-14 and column 4, lines 60-67].

9. As per claim 18, De Jong teaches the method as applied above. Furthermore, De Jong teaches the system in which the parameter is the number of the current communication session

in a series of communications between the first and second parties, and the number is stored as incremental data by each of the first and second parties to enable successive authentication and communication sessions [column 9, lines 1-14, 25-32 and column 4, lines 60-67].

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 2-8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Jong (US Patent No. 6,553,351 B1) in view of Cook et al. (hereinafter Cook) (US Patent No. 6,675,153 B1).

12. As per claim 2, De Jong teaches the system as applied above. Furthermore, De Jong teaches a value guaranteeing institution used with the first and second party subsystems [column 2, lines 42-58]. De Jong does not explicitly teach communication key is transmitted to a third party subsystem, which uses the communication key without decryption as an authentication key. However Cook teaches a transaction authorization system in which a third party subsystem used for authorizing transaction between a first and second party subsystems, in which communication data used without decryption [column 9, lines 24-48]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to incorporate a communication key transmitted to a third party subsystem, which uses the

communication key without decryption as an authentication key as per teachings of Cook into the authentication system of De Jong in order to authorize transactions between two subsystems securely.

13. As per claim 3, the combination of De Jong and Cook teaches the system as applied above. Furthermore, De Jong teaches approving the communication key if it is derived from any of various key data from the previously provided data pool related to the first party subsystem [column 3, lines 30-47 and column 4, lines 9-24].

14. As per claims 4 and 20, the combination of De Jong and Cook teaches the system as applied above. Furthermore, Cook teaches a transaction authorization system in which a third party subsystem used for authorizing transaction between a first and second party subsystems [column 9, lines 24-48].

15. As per claim 5, the combination of De Jong and Cook teaches the system as applied above. Furthermore, Cook teaches the system in which the second party subsystem confirms its approval of the transaction by seeking an approval from the first party subsystem, prior to transmitting the second party subsystem's approval to the third party subsystem [column 9, lines 24-48].

16. As per claim 6, the combination of De Jong and Cook teaches the system as applied above. Furthermore, De Jong teaches the system in which the first and second parties are privy to the key data [column 5, lines 19-24].

17. As per claim 7, the combination of De Jong and Cook teaches the system as applied above. Furthermore Cook teaches the system in which the first party subsystem is within a consumer's system, the second party subsystem is within a financial institution's system, the third party subsystem is within a merchant's system, and the key data is credit card data [column 9, lines 24-48].

18. As per claim 8, the combination of De Jong and Cook teaches the system as applied above. Furthermore, Cook teaches the system in which communication key but not the credit card data is transmitted by the first party subsystem over the internet to the second party subsystem, who in turn transmits it with a request to authorize the transaction to the third party subsystem [column 9, lines 24-48].

19. Claims 11-16 and 20-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over De Jong (US Patent No. 6,553,351 B1) in view of Cook et al. (hereinafter Cook) (US Patent No. 6,675,153 B1) as applied above and further in view of Schneier (Reference U).

20. As per claims 11, 12, 21 and 22, the combination of De Jong and Cook teaches the method as applied above. Furthermore, De Jong teaches an algorithm based on one-way hash function [column 8, lines 59-67 and column 9, lines 1-14]. However De Jong fails to teach operations of the algorithm. However it is well know to use different methods of encryption algorithm for encrypting data. For example Schneier teaches public-key algorithm mode used for a one-way hash function [pages 455-457]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement a method of

algorithm as per teachings of Schneier into the one-way hash function of De Jong in order to secure data by using an encryption algorithm that is secure from intruders.

21. As per claims 13, the combination of De Jong, Cook and Schneier teach the system as applied above. Furthermore, De Jong teaches the system in which the one way function includes credit card information as the context [column 8, lines 59-67 and column 9, lines 1-14].

22. As per claims 14, 15 and 23, the combination of De Jong, Cook and Schneier teach the system as applied above. Furthermore, De Jong teaches the system in which the encryption algorithm includes a unique context parameter that varies the communication key for each communication session, the key data being thereby indeterminable by an outside party subsystem who might monitor a series of such communication keys [column 9, lines 15-29].

23. As per claims 16, the combination of De Jong, Cook and Schneier teach the system as applied above. Furthermore, De Jong teaches the system in which the parameter is selected at a time known only to the parties intended to decrypt the communication key [column 5, lines 19-24].

24. As per claim 24, the combination of De Jong, Cook and Schneier teach the system as applied above. Furthermore De Jong teaches a value carrying device and a value receiving device [figure 1].

25. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over De Jong (US Patent No. 6,553,351 B1).

26. As per claim 19, De Jong teaches the system as applied to claim 17 above. However De Jong fails to teach the system in which the parameter is a date and time relating to the current communication session. However, Official notice is taken that it is well known to include date and time information in a parameter within a communication session for driving an encryption key in order to secure transactions between two entities by time stamping communications and preventing intruder actions.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Beemnet Dada

July 24, 2004